

HUMAN RESOURCES POLICY

Fauquier County, Virginia

Policy Title: Acceptable Computer System and Internet Use
Section No.: 52

Effective Date: 09/12/19
Supersedes Policy: 08/21/00

I. PURPOSE

Fauquier County provides a computer system, including access to the Internet, for the purpose of facilitating resource sharing, innovation and communication. The Board of Supervisors intends that the computer system be used:

(1) for the purposes of work, communication or research consistent with the Board of Supervisors' objectives;

(2) for legitimate County business; and

(3) consistent with the mission or administrative function of the County.

II. SCOPE

All users of Fauquier County's computer system have the responsibility to use this system in a considerate, ethical, and lawful manner. The purpose of this policy is to set forth the standards to which users must adhere in their use of the County's computer system. All users who are authorized to use the computer system, email and/or third-party websites, shall not be entitled to an expectation of privacy in the use of the system, and use shall be subject to monitoring by management at any time without notice or suspicion of wrongdoing.

III. DEFINITIONS

For purposes of this policy, the term “computer system” includes hardware, software, data communication lines and devices, terminals, printers, CD-ROM devices, tape drives, servers, mainframe and personal computers, mobile devices or other government furnished equipment or email, the Internet and other internal or external networks.

For purposes of this policy, the term “County” shall refer to Fauquier County Government.

For purposes of this policy, the term “account” shall mean the authorization to access computers or networks owned, leased or maintained by the County or accessed utilizing County assets.

For purposes of this policy, the term “All users” or “Users” shall refer to any individuals (i.e., employees, elected or appointed officials, contractors, consultants, temporary staff, volunteers, vendors, etc.) working on behalf of the Fauquier County Government or one of its sites or subsidiaries.

IV. **GOVERNING PRINCIPLES**

The Board of Supervisors has chosen to govern the use of Fauquier County's computer system through the establishment of this policy. The County's computer system is not a public forum. Violations of any of the provisions of this policy may result in disciplinary action, including but not limited to, the following: loss of accounts, loss of access, suspension or termination of employment, or legal action.

V. **RESPONSIBILITIES**

A. Use of Accounts

The County considers all accounts established by it as property of Fauquier County. The County authorizes the use of the accounts for specific purposes. Since accounts have real value, attempts to circumvent the account, system, to use the accounts of others without authorization, or to use accounts for other than their intended purposes are all forms of theft or misappropriation of public resources and shall be deemed a violation of this policy. An authorized user of an account may not use the account for personal gain, disclose its password, or otherwise make the account available to others who have not been authorized to use the account.

B. Integrity of the Network and Operating System

Users shall not utilize programs that harass other users of the facility, infiltrate the system and/or damage the software or hardware components of the system. Since all users depend on the availability and integrity of the network system, defects discovered in system accounting or system security shall be reported to the appropriate system administrator so that steps can be taken to investigate and solve the problem. Use of the electronic communication facilities to send fraudulent, harassing, obscene, indecent, profane, threatening, or intimidating messages is prohibited. Use of the electronic communications facilities to receive, review, or download obscene, indecent, profane, or illegal messages or materials is prohibited. Intentional damage of the system is prohibited.

C. Privacy of Other Users

Users shall not intentionally seek or provide information on, obtain copies of, or modify data files or programs belonging to other users without appropriate authorization. Attempts to gain unauthorized access to information of others without their permission will be treated as a violation of this policy. Unauthorized searching through directories to find unprotected information likewise is a violation. Users, when requested, shall cooperate with System Administrators in investigations of system abuse.

D. Use of Facilities and Equipment

Each network site has rules and regulations that govern the use of equipment and facilities at that site. Violation of facility rules and regulations shall be deemed a violation of this policy. Each site has operators, consultants, and/or supervisors who have been given the responsibility to supervise the use of that site. Users shall cooperate with site supervisors at all times.

E. Email and Communication Activities

Since malicious programs are often sent via email, users shall use extreme caution when opening ALL emails whether or not the "From" name is familiar and should employ email best practices including but not limited to:

- Compare From email address to valid address of any internal senders
- Compare From email address to valid company domain for external senders. (e.g., if the email is from Bank of America, be sure the From address is ExampleName@bankofamerica.com and not BadGuy@RandomBadDomain.com)
- Be wary of unsolicited/unexpected emails containing links or attachments (PDFs or .Zip, etc.) that are inconsistent with work responsibilities, whether internal or external or known or unknown. Think BEFORE you click.
 - Do NOT click links - first hover over them to see if path is legitimate
 - Do NOT click/download any unsolicited/unexpected attachments - first reach out to the sender via phone or a separate email to confirm legitimacy of information. If sender cannot confirm message, contact the System Administrator.
 - Check for misspellings or typos. Phishing emails often contain excessive misspelling or typos.
- Do not respond to spam email. Even if it is just to say "not interested". As this will confirm your email address as valid and could incite more emails.
- Encryption and/or password protection must be enabled when transferring sensitive or confidential data via email.

F. Internet Browsing

All users must employ internet browsing best practices, including but not limited to:

- Do NOT click any buttons-- "OK", "Agree", "No", "No, thanks" to any pop up. As those may trigger malware to run. Just use the "X" [right corner] to close; Alt+F4; or via task manager [using Ctrl+Alt+Delete -> Task manger-> right-click process and select "End"].

- Never install any unapproved software on any County system. Even if it is free.
- Avoid any URL/web address that does not end in .com, .us, .edu, .net, .gov, or .org unless the validity is absolute.
- Be sure to use "https" or only secured sites when entering any personally identifiable information (PII).

G. Social Media and Blogging Activities

- Blogging by employees, whether using County's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy and must be done in a professional and responsible manner, that does not otherwise violate County's policy, is not detrimental to County's best interests, and does not interfere with an employee's regular work duties. Blogging from County's systems is also subject to monitoring.
- County's Confidential Information policy also applies to blogging. As such, all users are prohibited from revealing any County confidential or proprietary information, or trade secrets when engaged in blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of County and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by any County policy.
- Employees may also not attribute personal statements, opinions or beliefs to County when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of County. Employees assume any and all risk associated with blogging.
- Any blogging activity must include a conspicuously placed statement on the blogging site stating that the views expressed are that of the individual and not to be associated with his/her employer.
- Use of County's trademarks, logos and any other County intellectual property in connection with any blogging activity is strictly prohibited.

VI. ADMINISTRATION AND ENFORCEMENT

- A. The County's computer system is not a public forum.
- B. Any communication or materials located on, disseminated through or used in conjunction with the computer system, including electronic mail or other files deleted from a user's account, may be monitored or read by County officials.
- C. Use of the computer system for research and communication purposes is a privilege, not a right. Users may be required to meet qualifications for use of the computer system for continued use of the system or employment.
- D. The failure of any user to follow the terms of this policy or any accompanying regulation may result in loss of computer system privileges, disciplinary action including termination of employment, and/or appropriate legal action.
- E. Fauquier County is not responsible for any information that may be lost, damaged, or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, Fauquier County will not be responsible for any unauthorized charges or fees resulting from access to the computer system.
- F. All use of Fauquier County's computer system shall be consistent with the Board of Supervisors' goal of promoting excellence by facilitating resource sharing, innovation and communication.

VII. AUTHORIZATION OF USE

- a. Each administrator, department manager, supervisor or employee whose duties include authorizing employees or volunteers to use of the computer system, shall ensure that these regulations have been discussed with the employee or volunteer prior to authorizing the use.
- b. Each elected or appointed board member, commissioner, or other official or user who receives authorization to utilize the County's computer system or email, who is not by other agreement bound by the County's personnel policies, shall sign an acknowledgment and agreement to act in accordance with and be bound by this policy prior to their first authorized use (Attachment 1).

VIII. COMPUTER SYSTEM USE – TERMS AND CONDITIONS

A. The following terms and conditions apply to any and all users of the County's computer system:

- **Acceptable Use:** Use of the County's computer system shall be: (1) for the purposes of work, communication or research; (2) consistent with the Board of Supervisors' policies; and (3) for legitimate County business.
- **Privilege:** The use of the County's computer system is a privilege, not a right. Therefore, personal use of County's computer system should be very limited. However, should the user decide to use the system for personal use, please use caution when entering their personally identifiable information (PII) such as bank account information, address, birth date, credit card information, etc. on any website. By no means should County's computer system be used to support a personal private business, whether "for-profit" or nonprofit. There is no expectation of privacy when using County computer systems and all users are expected to exercise good judgment regarding appropriate uses of County computer systems. Any user that makes personal use of County computer systems is assuming all risk associated with that activity including, but not limited to, disclosure of PII or financial loss. The County is not liable for any losses or damage that occurs to users as a result of personal use of County computer systems.

B. **Unacceptable Use**

Each user is responsible for his or her actions on the computer system. Prohibited conduct includes:

- using the network for any activity which results in a violation of copyright, license agreement or contract, trade secret, patent or other intellectual property;
- transmitting, sending, receiving, viewing or downloading any material in violation of any federal, state or local law;
- using the computer system for private financial or commercial gain;
- knowing and intentional waste of system resources, such as file space;
- gaining unauthorized access to resources or entities within or without the County system, or any form of hacking;
- gaining access to any data, server, or an account (whether secured or unsecured) for any purpose other than for conducting Fauquier County business, even if access is authorized;
- posting material authorized or created by another without his or her consent;
- using the computer system for commercial or private advertising;
- submitting, posting, publishing or displaying any obscene, profane, threatening, illegal, or other inappropriate material via the computer system;

- using the computer system without authorization, or while access privileges are suspended or revoked;
- vandalizing the computer system, including destroying data by creating or spreading viruses or by other means;
- introduction of malicious programs (i.e., viruses, worms, trojans, etc.) into the workstation, server, or network; or
- interfering with any workstation or network security tools or protocols (such as disabling anti-virus scanners).

C. ***Network Etiquette***

Each user is expected to abide by generally accepted rules of etiquette, including the following:

- Be polite;
- Users shall not forge, intercept or interfere with e-mail messages;
- Use appropriate language. The use of obscene, lewd, profane, threatening or disrespectful language is prohibited;
- Users shall not post personal contact information about themselves or others;
- Users shall respect the computer system's resource limits;
- Users shall not post chain letters or download large files;
- Users shall not use the computer system to disrupt others;
- Users shall not read, modify or delete data owned by others; and
- Users shall not use e-mail accounts of others without their consent.

D. ***Liability***

Fauquier County makes no warranties for the computer system it provides. County shall not be responsible or liable for any losses or damages to the user from use of the computer system, including, but not limited to, loss of data, non-delivery or missed delivery of information, or service interruptions. The County denies any responsibility for the accuracy or quality of information obtained through the computer system.

E. ***Security***

Computer system security is a high priority for the County. If any user identifies a security problem, the user shall notify the system administrator immediately. All users shall keep their passwords confidential and shall follow computer virus protection procedures. All users shall perform a screen lock on County systems when stepping away from the system. All users shall ensure the physical security of County systems by taking any reasonable precautionary measures to protect County systems from fire, flood, natural disasters, burglary, theft, and vandalism.

Policy Title:
Acceptable Computer System
And Internet Use

Section No.:
52

Effective Date:
August 21, 2000

F. ***Charges***

The County assumes no responsibility for any unauthorized charges or fees as a result of using the computer system, including telephone or long-distance charges.

Attachment 1

Authorization for Use of County Computer System

Other Authorized Users

I, _____, having been elected/appointed/employed (circle one)
to or by _____ (entity, board or commission name) hereby
acknowledge that I have read and understand the County's Acceptable Computer System and
Internet Use personnel policy (Section 52) and hereby agree to abide by and be subject to all of
its terms and conditions.

Signature

Date